Nota de prensa
29 de enero de 2026

En la categoría de Tecnologías de la Información y la Comunicación

Premio Fronteras del Conocimiento a Joan Daemen y Vincent Rijmen por diseñar el sistema criptográfico que protege la seguridad de dispositivos electrónicos y conexiones digitales en todo el mundo

- **Los ingenieros belgas crearon a finales del siglo pasado el llamado algoritmo de 'Rijndael' (fusionando sus dos apellidos),** que sigue siendo hoy el sistema estándar a escala internacional para proteger la seguridad y privacidad de internet, los ordenadores portátiles, los móviles, las conexiones wifi, los sistemas de mensajería digital, las tarjetas bancarias y el almacenamiento de datos en la nube, entre muchas otras aplicaciones

- **Durante el último cuarto de siglo, este sistema basado en "una profunda investigación sobre los fundamentos matemáticos de la criptografía"** se ha convertido en una tecnología que "sustenta la era digital actual", resalta el jurado, ya que gracias a ella "nuestro dinero permanece en nuestras cuentas bancarias, nuestros historiales médicos siguen siendo privados y nuestros mensajes solo llegan a las personas a las que queremos enviarlos"

- **Su contribución pionera constituye "un ejemplo paradigmático de cómo la teoría fundamental puede dar lugar a una tecnología que cambia el mundo"**, y a "aplicaciones prácticas que afectan a miles de millones de personas", concluye el jurado

El Premio Fundación BBVA Fronteras del Conocimiento en Tecnologías de la Información y la Comunicación ha sido concedido en su XVIII edición a los ingenieros Joan Daemen (Universidad Radboud de Nimega, Países Bajos) y Vincent Rijmen (Universidad Católica de Lovaina-KU Leuven, Bélgica, y Universidad de Bergen, Noruega) por diseñar las tecnologías criptográficas que "sustentan la era digital actual", en palabras del jurado, al proteger la seguridad de "millones de dispositivos conectados en todo el mundo".

En 1997, ambos investigadores belgas crearon un algoritmo bautizado como *Rijndael* —una combinación de sus dos apellidos— que pocos años después —2001, en EEUU, y 2005, a escala internacional— se convirtió en el estándar internacional utilizado para preservar la seguridad y

privacidad de las páginas de internet, los ordenadores portátiles, los móviles, las conexiones wifi, los sistemas de mensajería digital, las tarjetas bancarias y el almacenamiento de datos en la nube, entre muchas otras aplicaciones. Por ello, el jurado señala que a lo largo de los últimos 25 años el sistema criptográfico diseñado por los premiados "se ha convertido en una parte intrínseca de la vida cotidiana" en la sociedad global del siglo XXI.

Gracias a este algoritmo, basado en "una profunda investigación sobre los fundamentos matemáticos y algorítmicos de la criptografía", según resalta el acta, "nuestro dinero permanece en nuestras cuentas bancarias, nuestros historiales médicos siguen siendo privados y nuestros mensajes solo llegan a las personas a las que queremos enviarlos".

Al fin y al cabo, la criptografía constituye hoy "la columna vertebral de la confianza en el mundo digital", ya que "garantiza la confidencialidad, integridad y autenticidad de la información en todo, desde mensajes personales y transacciones con tarjetas de crédito hasta sistemas financieros globales". Sin esta tecnología tan fundamental, "no habría una identidad digital fiable, servicios en la nube ni dispositivos conectados; en definitiva, dejaríamos de tener una sociedad moderna.

El jurado también destaca el hecho de que que Daemen y Rijmen "tomaron la decisión crucial de dejar su algoritmo como código abierto, lo que permitió no solo la estandarización global, sino también la transparencia en la comunidad criptográfica: se enseña en todos los cursos del mundo en materia de seguridad informática y se puede examinar en busca de vulnerabilidades".

Por todo ello, concluye el acta, la contribución de Daemen y Rijmen "constituye un ejemplo paradigmático de cómo la teoría fundamental puede dar lugar a una tecnología que cambia el mundo y a aplicaciones prácticas que afectan a miles de millones de personas".

Para Ron Ho, vicepresidente corporativo de I+D en Hardware en Lattice Semiconductor (EEUU) y secretario del jurado, la vigencia global del sistema criptográfico creado por los galardonados "es una prueba del rigor científico, la apertura y la transparencia de ese algoritmo, y realmente ha sustentado todo lo que hacemos hoy en día como sociedad interconectada. Cada vez que visitas un sitio web, cada vez que compras algo, cada vez que vas al médico, estás utilizando estos principios básicos subyacentes. Por eso creo que ha sido muy importante para todos nosotros".

Joos Vandewalle, catedrático emérito del Departamento de Ingeniería Eléctrica de la Universidad Católica de Lovaina y experto en el campo de la criptografía, destaca que el algortimo *Rijndael* "ha

resistido 25 años de ataques por parte de investigadores famosos" que han intentado demostrar su vulnerabilidad. "Si quieres hacerte un nombre en criptografía, intentas romper los estándares de cifrado avanzados. Pero hasta ahora no se ha conseguido y todo parece indicar que tampoco se conseguirá en un futuro próximo".

Por su parte, Javier López —catedrático de Ciberseguridad de la Universidad de Málaga— recalca que, a lo largo del último cuarto de siglo, "nadie ha logrado debilitar sustancialmente" el algoritmo creado por los dos galardonados y que "además de seguro, es rápido y muy versátil y flexible, porque al permitir utilizar distintas longitudes de claves se puede adaptar a diversos niveles de seguridad". El profesor López, que coincidió con Rijmen en la Universidad Politécnica de Graz (Austria) y le invitó a participar como ponente en un congreso sobre criptografía celebrado en Málaga en 2004, considera que la contribución de los premiados es un buen ejemplo del alto nivel de la comunidad criptográfica europea: "En otros campos de la tecnología puede que en Europa vayamos por detrás, pero no en este área en la que el verdadero potencial reside en la capacidad intelectual de los investigadores".

Un concurso para elegir el algoritmo más rápido y seguro

Cuando Daemen y Rijmen comenzaron su carrera investigadora en los años 1990, la manera en la que se cifraba la información confidencial adolecía de cada vez más defectos. Después de 20 años de uso, el algoritmo denominado *Data Encryption Standard* o DES, promovido por el Instituto Nacional de Estándares y Tecnología (NIST) —el organismo que regula la ciberserguridad en EEUU— se estaba volviendo demasiado inseguro como para seguir cumpliendo su función. El NIST convocó un concurso para buscar un nuevo algoritmo más rápido y seguro que se convirtiera en el nuevo estándar a nivel internacional, pero los plazos para presentar las propuestas eran bastante apurados. "Joan [Daemen] y yo tuvimos suerte, porque nuestros doctorados trataban precisamente de ese tema", recuerda Rijmen.

En sus tesis doctorales, habían estudiado aspectos matemáticos de la criptografía que se aplicaban directamente al desarrollo de un mejor algoritmo de cifrado, y el concurso les motivó para traducir sus investigaciones a un sistema que se pudiera utilizar en la práctica. El algoritmo que presentaron, *Rijndael*, se sometió junto con el resto de propuestas a varios años de intentos por parte de toda la comunidad investigadora de romper su seguridad. *Rijndael* acabó ganando la competición y, en 2001, se convirtió en el estándar estadounidense —conocido como Advanced Encryption Standard, o AES— de cifrado de datos. Cuatro años más tarde, se adoptó como estándar internacional, que sigue vigente hoy en día.

29 de enero de 2026

"En comparación con otros competidores —continúa Rijmen—, teníamos un muy buen razonamiento matemático detrás, mientras que otros contaron con solo unos meses para diseñar el algoritmo completo desde cero. Así que la suerte jugó un papel, aunque, como dicen, la suerte llega a quien está preparado para usarla. Y nosotros estábamos preparados".

El algoritmo de 'Rijndael': seguro, rápido y matemáticamente elegante

El algoritmo de *Rijndael* sirve para cifrar datos, es decir, para transformar un mensaje legible por cualquiera en una cadena de caracteres aparentemente aleatorios y por tanto incomprensibles. Para lograrlo, se sustituyen fragmentos del mensaje original por otros nuevos mediante operaciones matemáticas que dictan cómo realizar esa sustitución —que, además, depende de una clave que solo conocen el emisor y el receptor deseado, y que sirve también para descifrar el mensaje—.

Para que un algoritmo de cifrado sea útil, tiene que ser no solo seguro, es decir, que sea auténticamente imposible cifrar y descifrar el mensaje sin conocer la clave, sino también rápido de ejecutar en cualquier dispositivo, ya que se emplea constantemente. El algoritmo de *Rijndael* cumple ambos requisitos y, para lograr una velocidad aún mayor, está integrado en los chips de aquellos dispositivos que protegen sus datos y comunicaciones de forma cotidiana, ya sean ordenadores, teléfonos móviles, puntos de acceso a conexiones wifi y hasta puertas y ventanas que se abren por control remoto.

La ubicuidad de este algoritmo, matiza Daemen, tiene también su lado negativo, ya que está tan extendido que es difícil pensar en cambiar a otro sistema de cifrado. "Como investigador, no me gusta esta faceta, porque frena el progreso científico. Pero, claro, como coautor de *Rijndael* estoy muy satisfecho". Con todo, el galardonado destaca que está mucho más orgulloso de la elegancia matemática de su algoritmo que de su éxito final. "Es un algoritmo muy simétrico, muy bonito. Eso es lo que trato de integrar en todo mi trabajo: simplicidad, simetría y belleza, un poco a la manera de Escher, que se esmeraba por dibujar algo bello y con mucha simetría y obtenía creaciones increíbles".

El esfuerzo colectivo, la clave del éxito en criptografía

En la era de los datos, eso sí, la importancia del algoritmo galardonado para la sociedad es innegable. "Cuando se empezaron a emplear los ordenadores", recuerda Rijmen, "se usaban como meras máquinas de escribir. Fue cuando las personas se empezaron a conectar a internet

que, de repente, cualquiera podía acceder a tu ordenador y, para gestionarlo, la seguridad se volvió imprescindible. En este sentido, actualmente se piensa que es mejor que exista un estándar internacional del que cualquiera puede comprobar la seguridad, en lugar de diluir estos esfuerzos si hay varios estándares, y nuestro algoritmo resulta ser el elegido. Y ahora se usa tantísimo porque dependemos cada vez más de los datos digitales", constata.

Efectivamente, hasta los años 1970, la seguridad de la información se limitaba al ámbito militar y de los servicios secretos, y fue solo con la proliferación de las comunicaciones electrónicas que comenzó a formarse una comunidad de personas dedicadas a la investigación en criptografía. "Fue el inicio del progreso en este campo —afirma Daemen—, porque permitió obtener una comunidad que compartía ideas. Algunas personas realizaban propuestas, otras las rompían, y así se obtenían resultados cada vez mejores".

Esta tradición se mantiene hoy en día y es la que ha permitido tener "un mejor conocimiento de la criptografía", resume Daemen, ya que "hasta entonces lo que había eran islas, el servicio secreto de cada país desarrollando sus propias herramientas. Así, se repiten los errores, mientras que al tener una sola comunidad son mucho menos frecuentes. Ahora, la comunidad ha crecido muchísimo y es imposible leer todos los artículos que se publican, así que hay una cierta fragmentación. Pero desde luego estamos mucho mejor ahora que en aquellos tiempos".

De hecho, esta colaboración de una gran comunidad es precisamente la que ha permitido mantener la vigencia del algoritmo de *Rijndael*. El gran avance se realizó gracias a las lecciones aprendidas a medida que el estándar anterior se quedaba obsoleto, ya que aquel fue el primero cuyos detalles se hicieron públicos. Sin embargo, se adoptó como estándar antes de que se empleara realmente en la práctica, y las vulnerabilidades no tardaron en aparecer. "A veces te crees que has tenido una buena idea, y matemáticamente funciona. Pero la gente comienza a usarla y te das cuenta de que no has pensado en ciertos aspectos. Esto es lo que sucedía con el estándar anterior, y nosotros pudimos usar toda aquella experiencia para construir algo mejor", explica Rijmen.

Cómo protegernos ante nuevos ataques en la era de la computación cuántica

El algoritmo galardonado ha demostrado ser seguro también ante ataques procedentes de un ordenador cuántico lo suficientemente potente. Aunque se debate lo cerca o lejos que pueda estar esa amenaza, las exigencias del NIST ya en los años 1990 contaban con el margen suficiente

como para que el AES haga frente a este tipo de ataques. Sí tendrá que cambiar, matizan los galardonados, otro tipo de criptografía, conocida como de clave pública, que se emplea por ejemplo para firmar digitalmente los documentos. Tras un nuevo concurso del NIST, en 2024 se eligieron tres estándares que permitirán proteger también esta faceta frente a ataques cuánticos.

Ahora, los premiados centran su investigación en perfeccionar la seguridad de los dispositivos que emplean su algoritmo. "El AES se define a nivel matemático y se puede demostrar que es irrompible —argumenta Rijmen—. Pero las operaciones matemáticas se realizan en ordenadores o en chips que usan energía y se calientan un poco cada vez que ejecutan el algoritmo. Ahora bien, todas estas señales (la energía que usan, el calor que emiten) delatan hasta cierto punto lo que sucede dentro de ese chip, y si eres capaz de medir todas estas cosas, tienes información sobre la función matemática que hace que sea un poco más fácil romperla". Para proteger los dispositivos contra este tipo de ataques, el galardonado estudia cómo lograr que el tiempo de computación, la potencia consumida, el calor emitido y cualquier factor que pueda ofrecer pistas indeseadas sea siempre el mismo o, al menos, que las pequeñas variaciones no permitan obtener información sobre la clave secreta del cifrado.

Por su parte, Daemen se centra en reducir el consumo energético de los algoritmos de cifrado, un aspecto clave para garantizar su funcionamiento en dispositivos cada vez más pequeños. "Con la explosión de datos que tenemos hoy en día, si quieres encriptar terabytes de datos por segundo tienes que minimizar el calor que produce esa operación. Pero en el plano opuesto, también interesa que el consumo de energía sea reducido en los dispositivos que funcionan con baterías, para que su carga dure mucho tiempo", alega. "El ejemplo típico —continúa— es un marcapasos que se pueda comunicar con el mundo exterior, pero tiene que estar protegido criptográficamente para que nadie lo pueda *hackear* a distancia".

Biografías de los premiados

Joan Daemen (Achel, Limburgo, Bélgica, 1965) obtuvo el título de Ingeniería Civil en Electrónica en KU Leuven (Bélgica) y se doctoró en la División de Seguridad Informática y Criptografía Industrial (COSIC, por sus siglas en inglés) de esa misma institución en 1995. Tras un breve periodo en la compañía Janssen, su trayectoria se orientó por completo a la ingeniería y arquitectura de seguridad, primero en Bacob Bank (1996) y a continuación en Banksys (1996-1998), Proton World (1998-2003) y STMicroelectronics (2003-2018), donde fue criptógrafo principal. En 2015 se incorporó a la Universidad Radboud (Nimega, Países Bajos) como

catedrático de Criptografía Simétrica en el Grupo de Seguridad Digital, que dirige desde 2019. Entre sus trabajos recientes figuran un proyecto concedido por el Consejo Europeo de Investigación para la iniciativa ESCADA, sobre los fundamentos de seguridad en criptografía simétrica, y un TOP Grant del Consejo Neerlandés de Investigación (NWO) sobre el diseño de criptografía simétrica para explotar de manera óptima los multiplicadores disponibles. Es copresidente del Programa Científico de Eurocrypt 2026.

Vincent Rijmen (Lovaina, Bélgica, 1970), titulado en Ingenieria Electrónica, se doctoró en la División de Seguridad Informática y Criptografía Industrial (COSIC) de KU Leuven en 1997 y continuó haciendo investigación en esta unidad del Departamento de Ingeniería Eléctrica (ESAT) hasta 2001. En 2001 se incorporó a la Universidad Técnica de Graz (Austria), donde fue catedrático de Criptología Aplicada. En 2007 regresó a KU Leuven, donde hoy es catedrático adscrito al COSIC y director del ESAT, cargos que compatibiliza con el de *Adjunct Professor* en el Centro Selmer de Comunicación Segura de la Universidad de Bergen (Noruega). Autor de aproximadamente 280 publicaciones y tres libros, es *Editor-in-Chief* del *Journal of Cryptology* y ha sido *Editor* de *Information Processing Letters*, *IET Information Security* y *Designs, Codes and Cryptography*. Ha sido copresidente del Programa Científico de Eurocrypt 2018 y 2019 y de otros congresos internacionales, así como director de Programa del Máster en Ingeniería Eléctrica de KU Leuven. Entre otras distinciones, es *fellow* del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y de la Asociación Internacional de Investigación Criptológica.

Nominadores

En esta edición se recibieron 38 nominaciones que incluyen un total de 36 candidatos. Los investigadores premiados fueron nominados por **Michel Abdalla**, científico de investigación sénior en Nexus, científico de investigación en CNRS y presidente de la Asociación Internacional de Investigación Criptológica (Estados Unidos); **Lejla Batina**, catedrática de Seguridad Digital en la Universidad Radboud (Países Bajos); **Guido Bertoni**, CEO de Security Pattern (Italia); **Claude Carlet,** catedrático emérito de Matemáticas en la Universidad París 8 (Francia); **Tor Helleseth**, catedrático emérito en el Departamento de Informática de la Universidad de Bergen (Noruega); **Seth Hoffert**, ingeniero de Desarrollo de Software, Advisor II (Estados Unidos); **Bart Jacobs**, catedrático de Seguridad, Privacidad e Identidad en la Universidad Radboud (Países Bajos); **Yves Moulart**, director del Centro de Diseño de Software de STMicroelectronics (Bélgica); **Michaël Peeters**, ingeniero principal sénior de Seguridad en STMicroelectronics (Bélgica); **Bart Preneel**, catedrático de Seguridad Informática y Criptografía Industrial en KU Leuven (Bélgica); **Gilles Van**

29 de enero de 2026

Assche, criptógrafo principal sénior en STMicroelectronics (Bélgica); y **Ronny Van Keer**, ingeniero principal de Diseño de Software en STMicroelectronics (Bélgica).

Jurado y Comité Técnico de Tecnologías de la Información y la Comunicación

El presidente del jurado de esta categoría ha sido **Oussama Khatib**, catedrático de Ciencia de la Computación y director del Centro de Robótica en la Universidad de Stanford (Estados Unidos); y su secretario, **Ron Ho,** vicepresidente corporativo de I+D en Hardware en Lattice Semiconductor (Estados Unidos).

Los vocales del jurado han sido **Regina Barzilay**, *School of Engineering Distinguished Professor* de Inteligencia Artificial y Salud en el Instituto Tecnológico de Massachusetts (Estados Unidos) y Becaria MacArthur; **Georg Gottlob**, catedrático de Informática en la Universidad de Calabria (Italia) y catedrático emérito de Informática en la Universidad de Oxford (Reino Unido); **Rudolf Kruse**, catedrático emérito en la Facultad de Ciencia de la Computación de la Universidad Otto von Guericke de Magdeburgo (Alemania); **Mario Piattini**, catedrático de Lenguajes y Sistemas Informáticos de la Universidad de Castilla-La Mancha (España); **Daniela Rus**, directora del Laboratorio de Ciencia de la Computación e Inteligencia Artificial (CSAIL) del Instituto Tecnológico de Massachusetts (Estados Unidos); **Bernhard Schölkopf**, director científico del Instituto ELLIS en Tubinga y director del Departamento de Inferencia Empírica del Instituto Max Planck de Sistemas Inteligentes (Alemania); y **Joos Vandewalle**, presidente de honor de la Real Academia Flamenca de Ciencias y Artes de Bélgica y catedrático emérito del Departamento de Ingeniería Eléctrica de la Universidad Católica de Lovaina (Bélgica).

En cuanto al **Comité Técnico de Apoyo**, ha estado coordinado por **Elena Cartea**, vicepresidenta adjunta de Áreas Científico-Técnicas del Consejo Superior de Investigaciones Científicas (CSIC), y por **José Javier Ramasco Sukia**, profesor de investigación en el Instituto de Física Interdisciplinar y Sistemas Complejos (IFISC, CSIC-UIB); e integrado por **Alberto Ibáñez Rodríguez**, científico titular en el Instituto de Tecnologías Físicas y de la Información Leonardo Torres Quevedo (ITEFI, CSIC); **Luis Fonseca Chácharo**, profesor de investigación y director del Instituto de Microelectrónica de Barcelona (IMB-CNM, CSIC); **Felip Manyà Serres**, investigador científico y vicedirector del Instituto de Investigación en Inteligencia Artificial (IIIA, CSIC); y **Teresa Serrano Gotarredona**, profesora de Investigación y directora del Instituto de Microelectrónica de Sevilla (IMSE-CNM, CSIC).

29 de enero de 2026

Sobre los Premios Fundación BBVA Fronteras del Conocimiento

La Fundación BBVA tiene entre sus focos de actividad el fomento de la investigación científica y la creación cultural de excelencia, así como el reconocimiento del talento.

Los Premios Fundación BBVA Fronteras del Conocimiento, dotados con 400.000 euros en cada una de sus ocho categorías, reconocen e incentivan contribuciones de singular impacto en las ciencias básicas, la biomedicina, las ciencias del medio ambiente y el cambio climático, las tecnologías de la información y la comunicación, las ciencias sociales, la economía, las humanidades y la música. El objetivo de los galardones, desde su creación en 2008, es celebrar y promover el valor del conocimiento como un bien público sin fronteras, que beneficia a toda la humanidad, siendo la mejor herramienta para afrontar los grandes desafíos globales de nuestro tiempo y ampliar la visión del mundo de cada persona. Sus ocho categorías se corresponden con el mapa del conocimiento del siglo XXI.

En esta familia de premios la Fundación BBVA cuenta con la colaboración de la principal organización pública española de investigación, el Consejo Superior de Investigaciones Científicas (CSIC), que designa Comités Técnicos de Apoyo, integrados por destacados especialistas del correspondiente ámbito de conocimiento, que llevan a cabo la primera valoración de las candidaturas, elevando al jurado una propuesta razonada de finalistas. El CSIC designa, además, la presidencia de cada uno de los ocho jurados en las ocho categorías de los premios y colabora en la designación de todos sus integrantes, contribuyendo así a garantizar la objetividad en el reconocimiento de la innovación y excelencia científica. La Presidencia del CSIC participa también de manera destacada en la ceremonia de entrega de los galardones que cada año se celebra en Bilbao, sede permanente de los Premios Fundación BBVA Fronteras del Conocimiento.

CONTACTO:
Departamento de Comunicación y Relaciones Institucionales
Tel. 91 374 52 10 / 91 374 81 73 / 91 537 37 69
comunicacion@fbbva.es
Para información adicional sobre la Fundación BBVA, puede visitar: www.fbbva.es