www.premiosfronterasdelconocimiento.es

Discurso de aceptación

18 de junio de 2026

Joan Daemen, galardonado en la categoría de Tecnologías de la Información y la Comunicación (XVIII edición)

En primer lugar, me gustaría agradecer a la Fundación BBVA la concesión de este premio a mi colega Vincent Rijmen y a mí mismo por nuestro trabajo en el campo de la criptografía. Quiero dar las gracias a todos los que nos han brindado su apoyo, orientación y ánimo a lo largo de este camino; ellos saben quiénes son.

Tradicionalmente, la criptografía es el arte de diseñar sistemas de criptografía —cifrados— para salvaguardar la confidencialidad y la autenticidad de las comunicaciones. Los cifrados bien diseñados pueden proteger los mensajes incluso frente a los intrusos más poderosos siempre que se mantengan en secreto las cadenas de caracteres breves, similares a contraseñas, llamadas claves. Durante milenios, la criptografía y el arte de descifrar códigos, es decir, el criptoanálisis —en conjunto, denominados criptología—, se mantuvieron bien custodiados y reservados a gobernantes, militares y diplomáticos, y con frecuencia desempeñaron una función crucial en la guerra. A consecuencia de todo ello, el progreso era lento y muchos de los conocimientos que tanto esfuerzo había costado adquirir se perdían con la muerte de los expertos o la caída de los imperios.

A mediados de los años setenta se produjo un cambio cuando el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos publicó el primer estándar criptográfico abierto: el Estándar de Cifrado de Datos (DES). A partir de ese momento, la criptología pasó a ser una disciplina científica abierta, lo que dio lugar a asombrosos avances en sus conocimientos. Desde principios de siglo, con el auge de Internet y, en general, la digitalización del mundo, la criptología se ha convertido en una disciplina de enorme importancia social. A partir de los años setenta, la investigación abierta dio lugar a una amplia variedad de algoritmos criptográficos. Muchos de ellos fueron descifrados poco después de publicarse, ya que los diseñadores,

comprensiblemente orgullosos de sus creaciones, suelen pasar por alto sutiles vulnerabilidades. Todavía no se ha demostrado nunca que ningún cifrado funcional sea seguro, y muchos creen que se trata de un ideal inalcanzable.

Entonces, ¿cómo generar confianza en un cifrado? Los avances en criptología surgen de un proceso disciplinado de ensayo y error dentro de la comunidad académica: se proponen cifrados, se analizan, se descifran, se corrigen y se vuelven a descifrar hasta que el ritmo de los nuevos ataques se ralentiza. Este ciclo —sustentado por los congresos (que someten los cifrados a revisiones por pares), las revistas especializadas y la colaboración abierta— ha demostrado ser extraordinariamente fructífero. Cada ataque aporta nuevos conocimientos y principios de diseño, y esto conduce a una sofisticación matemática cada vez mayor y a los robustos cifrados de hoy en día.

Cuando empecé mi doctorado en criptografía en 1988, aún estábamos muy lejos de contar con cifrados sólidos. El estándar DES dominaba la investigación sobre criptografía simétrica y, en la práctica, los gobiernos, los bancos y la industria confiaban en una versión mejorada de este: el Triple-DES. Todo indicaba que la situación seguiría igual en un futuro previsible. El Triple-DES era muy eficiente y parecía lo suficientemente seguro, pero, desde luego, no se podía calificar de elegante. Por eso, tras algunos intentos fallidos, decidí dedicar mi doctorado a intentar diseñar cifrados que fueran eficientes y seguros, pero más sencillos y elegantes. La clave de la elegancia era, y sigue siendo, la simetría, lo que me llevó a una serie de diseños de cifrado de índole más bien académica con los que sigo estando contento. Sabía que iba por buen camino cuando los revisores rechazaban mis artículos alegando solo que "estos cifrados parecen demasiado sencillos para ser seguros", sin aportar ninguna prueba de su vulnerabilidad.

Después de terminar el doctorado, cuando conseguí un puesto como consultor de *software* en una multinacional, se me ocurrió una idea que pensé podría dar lugar a algo grande, pero mi trabajo ya no tenía nada que ver con la criptografía y no me quedaban fuerzas para dedicarme a ello por mi cuenta después del horario laboral. Así que me puse en contacto con Vincent, con quien había colaborado muy satisfactoriamente en el grupo de investigación COSIC (Seguridad Informática y Criptografía Industrial) durante mi doctorado. Le propuse que desarrolláramos la idea juntos y, afortunadamente, dijo que sí. Sin mi iniciativa y la respuesta afirmativa de Vincent, nuestras vidas probablemente hubieran tomado un rumbo muy distinto. Nuestra colaboración dio lugar a una serie de artículos en los que presentamos varios sistemas de cifrado en los años 1996 y 1997.

Entonces ocurrió algo inesperado: nos llegaron rumores de que el NIST tenía previsto convocar un concurso abierto para hallar un sucesor del DES y, efectivamente, así lo hicieron; lo llamaron el concurso del Estándar de Cifrado Avanzado (AES). El NIST iba a encargarse de organizarlo, pero todo el trabajo (diseños, criptoanálisis, comparaciones) correría a cargo de la comunidad académica, y los participantes debían abstenerse de solicitar patentes.

Los algoritmos de cifrado que publicamos en 1996 y 1997 ya cumplían los requisitos del NIST, por lo que solo tuvimos que adaptar algunos detalles para presentar nuestra propuesta. Buscando un nombre que combinara nuestros

apellidos, elegimos Rijndael. Competíamos con otros 14 equipos, varios de ellos estadounidenses, y, para nuestra sorpresa, el NIST solo empleó argumentos técnicos en su selección. En octubre de 2000, el NIST anunció que Rijndael era el ganador del AES.

El concurso del AES fue una magnífica iniciativa del NIST, al que hasta ese momento la comunidad académica miraba con recelo al verlo como una filial de la Agencia de Seguridad Nacional (NSA). Tras el concurso del AES, el NIST pasó a ser considerado un colaborador fundamental en el proceso académico, y posteriormente organizó más concursos abiertos parecidos.

Creemos poder afirmar que nuestro invento, Rijndael, y los principios de diseño en los que se basa supusieron un avance crucial en el campo de la criptografía. En los veinticinco años transcurridos desde que el NIST estandarizara Rijndael al seleccionarlo como AES, han aparecido numerosos artículos sobre el criptoanálisis y las interesantes propiedades de Rijndael como AES, y en repetidas ocasiones se ha señalado que parece demasiado sencillo para ser seguro. Aun así, no se han publicado ataques efectuados en la práctica, y con el paso de los años el AES, ya convertido en el cifrado que goza de mayor confianza en todo el mundo, ha inspirado un sinfín de trabajos posteriores.