

Vincent Rijmen on CIO.

2009 marks 60 years of computer cryptography and CIO takes a tour of the history of secure communication:

CIO Blast from the Past - 60 years of cryptography click [here](#) to view the full slideshow

By [Rodney Gedda](#) 18 September, 2009

"2009 marks 60 years since the advent of modern cryptography. It was back in October 1949 when mathematician Claude Shannon published a paper on Communication Theory of Secrecy Systems. According to his employer at the time, Bell Labs, the work transformed cryptography from an art to a science and is generally considered the foundation of modern cryptography. Since then significant developments in secure communications have continued, particularly with the advent of the Internet and Web. CIO has a pictorial representation of the past six decades of research and development in encryption technology. Highlights include the design of the first quantum cryptography protocol by Charles Bennett and Gilles Brassard in 1984, and the EFF's 'Deep Crack' DES code breaker of 1998."

(Slide 15)

2000s: Encryption begins to open up as the US government relaxes restrictions on the export of cryptography and RSA Security releases its RSA algorithm into the public domain. A year later the Rijndael algorithm designed by Vincent Rijmen (pictured) and Joan Daemen becomes the US Advanced Encryption Standard (AES).

Prof. ir. dr. V. Rijmen is professor at ESAT-SCD-COSIC at K.U.Leuven