A short history of RSA

In 1976, Whitfield Diffie and Martin Hellman published a revolutionary paper titled "New Directions in Cryptography." Together with Ralph Merkle, the three researchers laid the foundations of the so-called "public-key cryptography."

Until that year, it was well accepted that encryption simply could not be done without first sharing a secret key. In 1976, "secret-key cryptography" seemed the only way to go.

Diffie, Hellman, and Merkle introduced three fundamental public-key (or asymmetric) primitives: *public-key encryption*, *digital signature*, and *key exchange*. However, they presented only the mathematical implementation of the key-exchange protocol, known as "Diffie-Hellman key exchange". It was the first practical method for establishing a shared secret over an unprotected communications channel.

A year later (1977), Ron Rivest, Adi Shamir, and Len Adleman proposed the first *public-key encryption scheme* (and also a digital signature scheme) based on the hardness of factorization. The scheme is known as RSA, from the initials of its proponents.

In the linked photo, from left to right: Shamir, Rivest, Adleman in MIT
https://people.csail.mit.edu/rivest/photos/rsa-photo.jpeg

Read about the origin of the RSA scheme
in the excerpt of the chapter "prime time" of
Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age,
a book about cryptography written by Steven Levy.

The excerpt is available upon request at identitiespr@gmail.com

Co-funded by the Erasmus+ Programme of the European Union
Grant Agreement n°2019-1-IT02-KA203-063184