

Adi Shamir (Institut Weizmann)

Adi Shamir holds a PhD degree in Computer Science from the Weizmann Institute. After a year postdoc at the University of Warwick, he did research at MIT before returning to be a member of the faculty of Mathematics and Computer Science at the Weizmann Institute. Starting in 2006, he is also an invited professor at École Normale Supérieure in Paris.

He is a co-inventor of the RSA cryptosystem. In addition, his contributions to cryptography include the Shamir secret sharing scheme, the breaking of the Merkle-Hellman knapsack cryptosystem, visual cryptography, and the TWIRL and TWINKLE factoring devices. Together with Eli Biham, he discovered differential cryptanalysis, a general method for attacking block ciphers. (It later emerged that differential cryptanalysis was already known — and kept a secret — by both IBM and the NSA.) He has also made contributions to computer science outside of cryptography, such as showing the equivalence of the complexity classes PSPACE and IP.

He has received a number of awards, including the 2002 ACM Turing Award, together with Rivest and Adleman, the Paris Kanellakis Theory and Practice Award; the UAP Scientific Prize, the Vatican's PIUS XI Gold Medal, the IEEE Koji Kobayashi Computers and Communications Award; and the Israel Prize, in 2008, for computer sciences.