



Les personnalités de l'Informatique et de la Science du Numérique, Rivest, Shamir et Adleman


Ronald Rivest, 1947

 Ronald Rivest est diplômé de l'université Yale en 1969 et docteur de l'université Stanford en 1974. Il rejoint les laboratoires du MIT où il fonde un groupe travaillant sur la sécurité de l'information et la cryptographie.

Adi Shamir, 1952

 Adi Shamir est né en 1952 à Tel Aviv. Shamir reçoit un BS en mathématiques à l'université de Tel Aviv en 1973 suivi d'un MSc et d'un doctorat en informatique à l'Institut Weizmann.

Leonard Adleman, 1945

 Né en Californie, Adleman grandit à San Francisco et étudie à l'université de Californie à Berkeley. Il décroche un doctorat en 1976. En 1994, son article "Molecular Computation of Solutions To Combinatorial Problems" décrit l'utilisation expérimentale de l'ADN dans les systèmes informatiques.

Le chiffrement RSA

Le nom du chiffrement RSA vient du nom de ses créateur (Rivest Shanir Adleman) qui ont reçu le prix de turing (l'équivalent du prix Nobel en informatique) en 2002. Le chiffrement RSA est un algorithme de cryptographie à clé publique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. L'algorithme utilise deux clés : une clé publique qui permet de chiffrer des données et une clé privée qui permet de déchiffrer des données. La clé privée appartient à la personne qui reçoit les données et la clé publique appartient à ceux envoient des données. La clé privée ne peut pas être retrouvée à partir de la clé publique.

En savoir plus

- [Le chiffrement RSA](#)
- [Ronald Rivest](#)
- [Adi Shamir](#)
- [Leonard Adleman](#)