



# Invention du RSA

1977



## Invention du RSA

Un des premiers algorithmes de chiffrement asymétrique, à la base de la sécurité des communications modernes. En 1977, Rivest, Shamir et Adleman ont développé l'algorithme RSA. Il utilise une paire de clés (une publique, une privée). La clé publique chiffre un message, qui ne peut être déchiffré qu'avec la clé privée. Ce principe est l'inverse de la cryptographie symétrique.

### 🧩 CONCEPT CLÉ

L'algorithme RSA permet la communication sécurisée entre deux personnes qui ne se sont jamais rencontrées. Ce concept de cryptographie asymétrique est la base de toute la cybersécurité moderne, des transactions bancaires en ligne aux VPN.