

RSA

RSA

Historique

- Inventé par Rivest, Shamir et Adleman dans les années 70s
- Une des premières solutions au problème d'établissement de clé avec Diffie-Hellman
- Initialement présenté comme un algorithme de signature digitale
- Tous deux encore largement utilisés sur internet pour la communication https
- Rivest et Adleman ont aussi introduit le concept de privacy homomorphisms
- La sécurité repose sur la difficulté réputée de la factorization entière