Systèmes à clés publiques

Pr.: Rendre impossible la construction de la clé de déchiffrement à partir de la clé de chiffrement.
- clé publique de chiffrement,
- clé privé de déchiffrement.

Rivest, Shamir et Adleman :(1977) factorisation des grands nombres ;

Rabin : factorisation des grands nombres ;

Merkle-Hellman : problème du sac-à-dos ;

McEliece : théorie algébrique des codes ;

ElGamal : logarithme discret dans un corps fini ;

Chor-Rivest : problème du sac-à-dos.