Le système RSA (1977) est un cryptosystème qui repose sur le problème de factorisation des grands entiers. C’est sans doute le plus populaire des systèmes à clés publiques.

La clé privée est constituée de deux nombres premiers p et q et d’un entier d premier avec   
φ(n)=(p-1)\*(q-1). La clé publique est constituée du produit n de p et q et d’un entier e inverse de d modulo φ(n).

L’ensemble des messages est l’ensemble Un des éléments inversibles modulo n.

L’opération de chiffrement est l’élévation à la puissance e modulo n. L’entier e étant l’exposant public.

L’opération de déchiffrement est l’élévation à la puissance d. L’entier d étant l’exposant privé.

D’après le théorème d’Euler, la composition de ces deux opérations est l’identité.

Le principe de la signature RSA est d’inverser les rôles des exposants e et d par rapport à leur utilisation dans le schéma de chiffrement. L’exposant privé d sert à chiffrer le condensé h du message. Seul le détenteur de la clé privée peut le faire. La signature est le résultat de ce chiffrement : σ=h^d. La vérification consiste à vérifier que σ^e=h.

Algorithme Rho de Pollard (1975)

L’idée de l’algorithme Rho et que si on parvient à trouver deux entiers distincts x et x′ inférieurs à n et tels que x≡x′ [p], alors x−x′ est multiple de p. Comme n est également multiple de p, le PGCD de x−x′ et n sera multiple de p, ce qui signifie qu’il sera égal à p ou n. Ainsi, on teste successivement des paires (x,x′) d’entiers de [0,n−1] jusqu’à trouver une paire telle que le PGCD de x−x′ et n est supérieur à 1 mais inférieur à n.

Complexité : 0(n^(1/4))

Crible algébrique

Algorithme le plus efficace actuellement mais difficile à implémenter dont la complexité est sous-exponentielle.