La sécurité est basée sur le concept :

Déf Une fonction f est à sens unique (one-way function) si

1. $y = f(x)$ est facile à calculer
2. $x = f^{-1}(y)$ est difficile à calculer.

Ex : RSA est basée sur le fait que si p, q sont entiers premiers, il est facile de calculer $y = p \cdot q$, mais il est difficile de retrouver la factorisation de y : problème de factorisation

Rq. 1) La notion de certificat relie la clé publique à B :

authentification

2) Un cryptosystème a un niveau de sécurité de n bits si le meilleur algorithme d'attaque exige 2^n étapes de calcul. (voir table livre Understanding cryptography de Paar et Pelzl, page 156)