§3. Cryptographie à clé publique basée sur le logarithme discret (LD)

RSA est basé sur le problème de la factorisation d'entiers qui est une fonction à sens unique. Une autre fonction à sens unique est le logarithme discret. (PLD) :

> (PLD) en général :
> soit G un groupe cyclique fini de cardinal n.
> soit $\alpha \in G$ un élément primitif de G, et soit $\beta \in G$.
> le PLD est de trouver x, $1 \leq x \leq n$ tq :
> $\beta = \alpha^x$, noté $x = \log_\alpha \beta$.

Le Protocole Diffie-Hellman d'Echanges de clés, le cryptosystème ELGAMAL (ainsi que la signature numérique) sont basés sur le PLD, et on peut étendre à plusieurs structures algébrique-Géométriques. telle les courbes elliptiques.