- Malléabilité :

O observe (k_E, y) et le remplace par :

$$(k_E, \lambda y) \quad \text{où} \quad \lambda \in \mathbb{N}.$$

B calcule :

$$d_{k_{prB}}(k_E, \lambda y) = \lambda \cdot y \cdot k_n^{-1}(p).$$

$$= \lambda \cdot (x \cdot k_n) \cdot k_n^{-1}(p)$$

$$= \lambda x \quad (\text{mod } p)$$

et le message de départ x est multiplié par λ.

($\Rightarrow$ padding).

Comme RSA.

§5. Cryptographie à base de Courbes elliptiques (ECC)

ECC (Elliptic Curve Cryptography) est basé sur le LD. dans le groupe-pour-jacent. Et donc les protocoles DH sont aussi valables. L'un des intérêt de ECC est qu'on a une meilleur sécurité avec des opérandes plus courts. (comparé à RSA). On verra ici le principe de fonctionnement (sans trop détailler les aspects mathématiques). Une large bibliographie existe. On verra aussi, une fois absorbé les Concepts de base, comment instaurer la cryptographie IBE (Identity Based Encryption) à la fin.