Remarques. Pour l'infrastructure noter que le Protocole DH exige de trouver p premier (voir test de primalité, § RSA) et aussi on fait l'exponentiation modulaire rapidement. Aussi le groupe cyclique fini G est ici $\mathbb{Z}_p^*$ de cardinal $p-1$. ☒.

(3.2) Attaques du P.L.D.

(3.2.1) Algorithmes génériques.

Utilise seulement la loi de groupes et non pas la structure particulière du groupe.

A1 • Recherche exhaustive !

Dans G, on teste :

$$\alpha^1 \overset{?}{=} \beta,\ \alpha^2 \overset{?}{=} \beta,\ \dots,\ \alpha^x = \beta.$$

$\Rightarrow$ temps $O(|G|)$.

par exemple si $G = \mathbb{Z}_p^*$, $|G| = p-1$.

on prend $p \simeq 2^{80}$ pour éviter l'attaque.

A2 • Baby-step Giant step de Shanks..!

C'est un algorithme meilleur que A1 utilisant un compromis espace / temps. Supposons que $x = \log_\alpha \beta$.

On écrit $x = x_g m + x_b$. $0 \le x_g, x_b < m$.

où $m = \lceil \sqrt{|G|} \rceil$