A4. Algorithme de Pohlig-Hellman

Basé sur le théorème chinois, il exploite une factorisation possible du groupe G en conjonction avec l'un des algorithmes A_i ($i \geq 3$).

Soit $|G| = p_1^{e_1} \cdots p_l^{e_l}$.

Au lieu de calculer $x = \log_\alpha \beta$, on calcule un L.D. plus petit $x_i \equiv x \bmod p_i^{e_i}$ dans un sous-groupe d'ordre $p_i^{e_i}$; ensuite on utilise le théorème chinois pour déduire une solution. Chaque P.L.D dans les sous-groupes est calculé par A2 ou A3.

(3.2.2.) Algorithmes non génériques : méthode d'index.

La méthode d'index calcule le L.D. dans certains groupes spécifiques comme $\mathbb{Z}_p^*$ et $GF(2^m)^*$ et donne lieu à des algorithmes sous-exponentiel.

(3.2.3) Sécurité du protocole d'Echange DH.

O. veut calculer k_{AB}, connaissant α, p et il peut obtenir A et B ($= k_{pub,A}$ et $k_{pub,B}$). Est-il capable de calculer $k = \alpha^{AB}$ (problème PDH).

PDH. Soit G groupe cyclique fini d'ordre n, $\alpha \in G$ primitive, et $A = \alpha^a$, $b = \alpha^b$ dans G.

Trouver α^{ab} ?