PKCS#3

Diffie-Hellman Key-Agreement Standard

L'échange de clé Diffie-Hellman est une méthode par laquelle 2 personnes peuvent se mettre d'accord sur un nombre qu'ils peuvent utiliser pour chiffrer des données.

Exemple

1. 2 utilisateurs A et B choisisent un nombre premier **p** et une base **g** : **p=23**, et **g=3**
2. L'utilisateur A choisi un nombre secret **a=6**
3. L'utilisateur A envoie la valeur $\mathbf{A = g^a \ [mod\ p] = 3^6\ [23] = 16}$
4. L'utilisateur B choisit un nombre secret **b=15**
5. L'utilisateur B envoie la valeur $\mathbf{B = g^b \ [mod\ p] = 3^{15}\ [23] = 12}$
6. L'utilisateur A calcule la clé secrète $\mathbf{K : (g^b \ [mod\ p])^a \ [mod\ p] = 12^6\ [23] = 9}$
7. L'utilisateur B calcule la clé secrète $\mathbf{K : (g^a \ [mod\ p])^b \ [mod\ p] = 16^{15}\ [23] = 9}$

Il est nécessaire d'utiliser des nombres suffisamment grand pour éviter une attaque par recherche exhaustive.

Diffie-Hellman est vulnérable aux attaques MITM. Pour parer à cette attaque, on peut signer les échanges avec une paire de clés asymétriques.