Protocole d'échange de clefs de Diffie-Hellman

Alice et Bob veulent partager une clef secrète K: On suppose que les données G; |n |= G et g sont publiques.

- Alice choisit un entier $1 \leq a \leq n-1$ au hasard.
- Alice calcule $A = g^a$ et l'envoie à Bob.
- Bob choisit un entier $1 \leq b \leq n-1$ au hasard.
- Bob calcule $B = g^b$ et l'envoie à Alice.
- Alice est en mesure de calculer B^a et Bob de calculer A^b. La clef commune est donc : $K = g^{ab} = A^b = B^a$:

Exemple :

1. Alice et Bob choisissent un nombre premier p et une base g: exemple, p = 23 et g = 3.
2. Alice choisit un nombre secret a = 6.
3. Elle envoie à Bob la valeur $g^a \bmod p = 36 \bmod 23 = 16$.
4. Bob choisit à son tour un nombre secret b = 15.
5. Bob envoie à Alice la valeur $g^b \bmod p = 315 \bmod 23 = 12$.
6. Alice peut maintenant calculer la clé secrète : $(g^b \bmod p)^a \bmod p = (12)^6 = 126 \bmod 23 = 9$
7. Bob fait de même et obtient la même clé qu'Alice : $(g^a \bmod p)^b \bmod p = (16)^{15} = 1615 \bmod 23 = 9$.

Exercice 1 : faites tourner l'algorithme d'échange de clé de Diffie-Hellman avec les valeurs suivantes

- p = 11 comme nombre premier
- g = 2 comme générateur de Z/pZ
- a = 4 comme nombre secret choisi par Alice
- b = 8 comme nombre secret pour Bob

Détaillez les calculs en mettant en avant les messages échangés par Alice et Bob. Quelle est-la clé ainsi obtenue ? .

Exercice 2 : Supposons qu'Alice et Bob partagent p = 233 et g = 45.

Si Alice choisit a = 11 et Bob b = 20 ; alors : Quelle est leur clef secrète commune ?