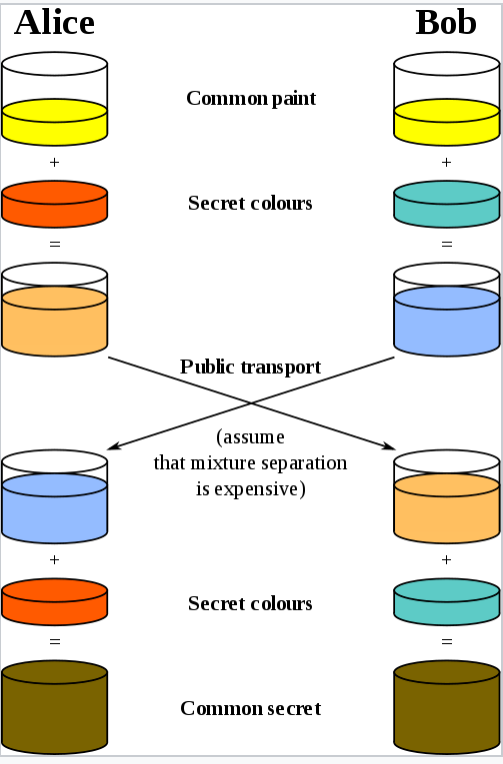


Diffie-Hellman is one of the common key exchange used worldwide nowadays. So the picture below would be much easier for understanding the concept behind Diffie-Hellman.



1. [Alice and Bob](https://en.wikipedia.org/wiki/Alice_and_Bob) publicly agree to use a modulus *p* = 23 and base *g* = 5 (which is a primitive root modulo 23).
2. Alice chooses a secret integer ***a*** = 4, then sends Bob *A* = *g****a*** mod *p*
   * *A* = 5**4** mod 23 = 4
3. Bob chooses a secret integer ***b*** = 3, then sends Alice *B* = *g****b*** mod *p*
   * *B* = 5**3** mod 23 = 10
4. Alice computes ***s*** = *B****a*** mod *p*
   * ***s*** = 10**4** mod 23 = 18
5. Bob computes ***s*** = *A****b*** mod *p*
   * ***s*** = 4**3** mod 23 = 18
6. Alice and Bob now share a secret (the number 18).

