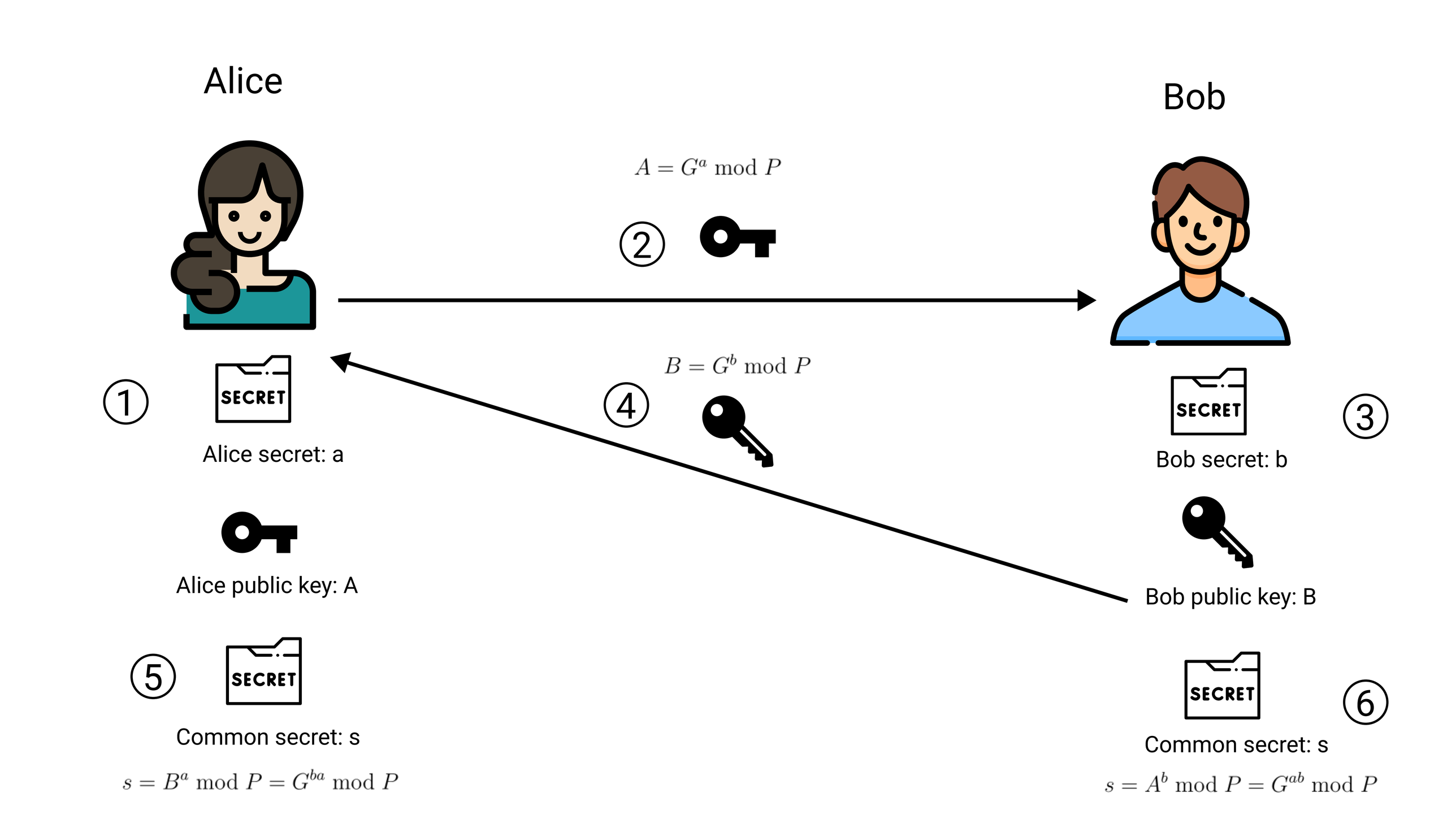
Alice
Bob
$A = G^a \bmod P$
2
$B = G^b \bmod P$
4
1
SECRET
Alice secret: a
SECRET
Bob secret: b
3
Alice public key: A
Bob public key: B
5
SECRET
Common secret: s
$s = B^a \bmod P = G^{ba} \bmod P$
SECRET
Common secret: s
6
$s = A^b \bmod P = G^{ab} \bmod P$