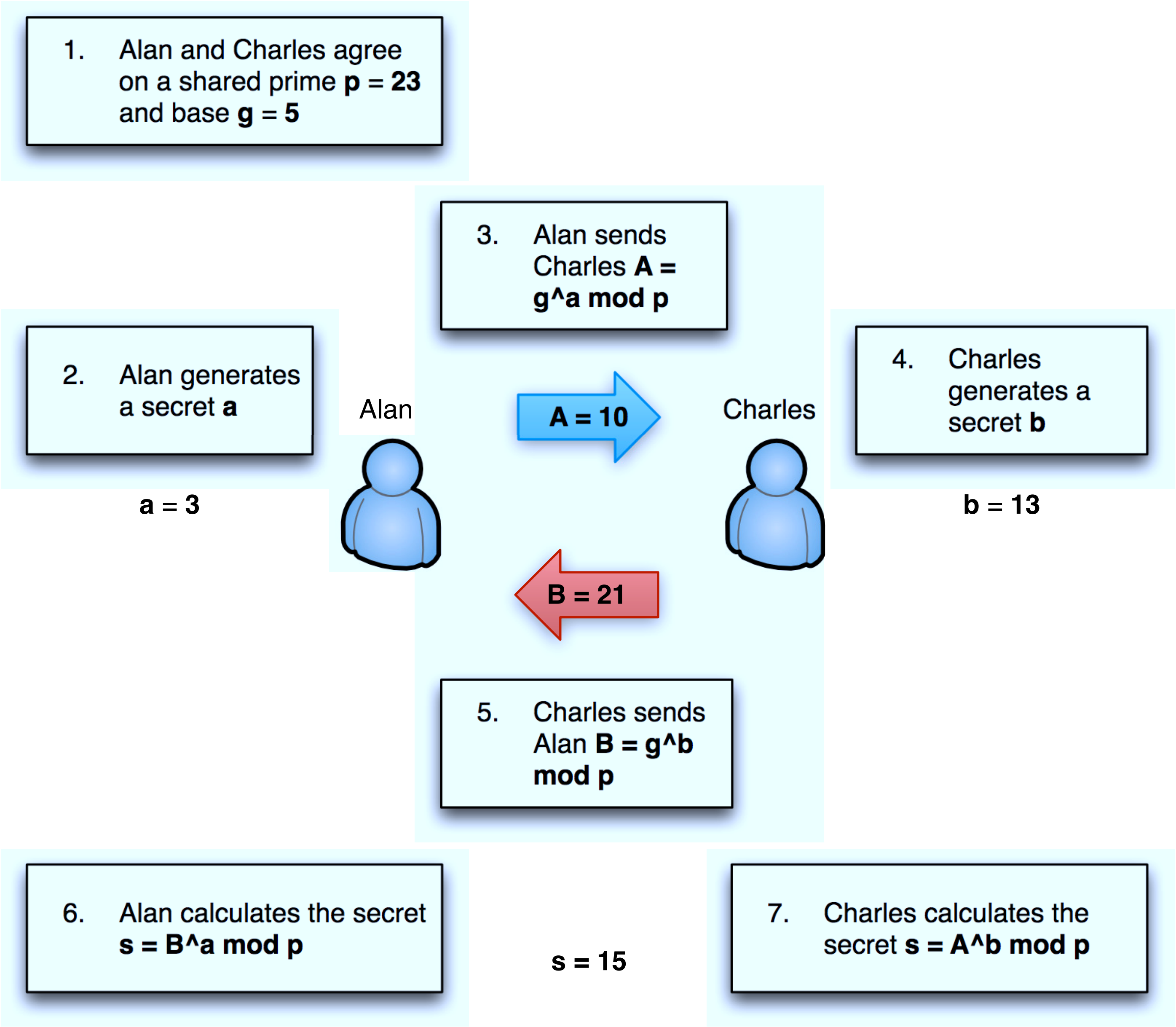

1. Alan and Charles agree on a shared prime **p** = **23** and base **g** = **5**

2. Alan generates a secret **a**

a = **3**

3. Alan sends Charles **A = g^a mod p**

4. Charles generates a secret **b**

b = **13**

5. Charles sends Alan **B = g^b mod p**

6. Alan calculates the secret **s = B^a mod p**

7. Charles calculates the secret **s = A^b mod p**

s = 15

Since **g^Ab = g^Ba**, both Alan and Charles get the same value, but an attacker knowing only **p**, **g**, **A** and **B** cannot calculate **s** without **a** or **b**