Diffie-Hellman key exchange

- Alice computes $s=g^{ba} \bmod p$. Bob computes $s=g^{ab} \bmod p$.
- Example: Alice and Bob agree to use p=23 and g=5 (publicly). Alice secretly uses a=6, and Bob secretly chooses b=15.

Alice sends to Bob $A = g^a \bmod p = 5^6 \bmod 23 = 8$

Bob sends to Alice $B = g^b \bmod p = 5^{15} \bmod 23 = 19$

Alice computes $s = B^a \bmod p = 19^6 \bmod 23 = 2$

Bob computes $s = A^b \bmod p = 8^{15} \bmod 23 = 2$